AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A countermeasure method in an electronic component using a cryptographic algorithm that comprises multiple successive rounds of operation with a secret key, wherein at least one of said rounds is implemented with a first manipulation means for supplying an output data item from an input data item, and the output data item is manipulated by means of instructions, and wherein at least one other round of said algorithm is implemented with other manipulation means for supplying output data, so that the output data item is unpredictable, said other manipulation means being obtained from said first manipulation means by performing an exclusive OR operation on said first manipulation means with a random value, and wherein each round using manipulation means for supplying an output data item from an input data item, the output data item being manipulated by instructions in at least a first three rounds and at least a last three rounds, and wherein said method includes the steps of forming a first group comprising at least the first three rounds and another group comprising at least the last three rounds, and implementing the first group and the last group with an execution sequence using the other manipulation means in at least some rounds.

2. (Canceled)

3. (Currently Amended) A countermeasure method according to Claim [[2]] 1, wherein four groups each of four successive rounds are formed, and said execution sequence is applied at least to the first group and to the last group.

4. (Previously Presented) A countermeasure method according to Claim 3, wherein said sequence is executed in each of the groups.

5. (Currently Amended) A countermeasure method according to Claim [[2]] 1, wherein said execution sequence is applied to a first group formed from the first three rounds and to a last group formed by the last three rounds.

6. (Previously Presented) A countermeasure method according to claim 1, wherein each execution of the algorithm includes the steps of drawing a random value and calculating said other manipulation means.

7. (Previously Presented) A countermeasure method according to claim 1 wherein said manipulation means are tables of constants.

8. (Previously Presented) A countermeasure method according to claim 1 wherein said manipulation means are used in combination with an additional exclusive OR operation with a value based upon the random value.

9 - 10. (Canceled)

11. (Previously Presented) The method of claim 1 wherein said random value is derived from one or both of the input and output data of said first manipulation means.

12. (Currently Amended) An electronic security component having a countermeasure against attacks on a secret key cryptography technique in which data is manipulated during multiple successive rounds of a cryptography algorithm, said component comprising:

a program memory having stored therein a first manipulating means that produces an output value from an input value;

means for generating a random value,

means for calculating at least one other manipulating means by combining said first manipulating means with said random value, and

a processor that executes said cryptography algorithm using said first manipulating means during some of said multiple rounds and said other manipulating means during other rounds of said algorithm, wherein each round using the manipulating means that produces an output value from an input value, the output value being manipulated by instructions in at least a first three rounds and at least a last three rounds, said algorithm further comprising the steps of forming a first group comprising at least the first three rounds and another group comprising at least the last three rounds, and implementing the first group and the last group with an execution sequence using the manipulating means in at least some rounds.

13. (Previously Presented) The electronic security component of claim 12, wherein said first and said other manipulating means each comprise a table of constants.

14. (Previously Presented) The electronic security component of claim 12, wherein said cryptography technique comprises a DES algorithm that is executed in multiple rounds.

15. (Previously Presented) The electronic security component of claim 12, wherein said component is a chip card.